ALPHACAPTURE
PROTOCOL

Tokenize Alpha

Build applications to prove performance, distribute and use alpha; for any asset; ideas or real trades.

By Louise Courtman and Cynan Rhodes (July 16th 2024)

Abstract

Traditional Finance (TradFi) investment management[1] – the buying or selling of assets on behalf of others, with the purpose of making a profitable return - exists within a regulated framework controlled by centralized intermediaries. It is maximally extractive, in terms of fees, and minimally inclusive, in terms of who can provide and who can access services.

Decentralized Finance (DeFi) investment management (whilst in DeFi, the term asset or investment management can mean the management of assets on one's own behalf, we are not concerned with that here; only with the management of assets on behalf of others) risks heading in the same direction. DeFi alternatives to date are skeuomorphic[2], designed almost exclusively on traditional, centralized models. It is inevitable that such solutions will be regulated in some way, which will lead to a model that very closely resembles the exact model that DeFi is trying to change.

Skeuomorphic DeFi investment management does not make use of all the unique capabilities of web3 to design a new framework for investment management that can deliver expertise and ease, but in a fully decentralized way, without the requirement to be regulated, without intermediaries, and not just for digital, but for traditional assets as well. It misses the incredible opportunity web3 offers to build a better, fairer investing system for the future.

What is needed is a web3 native investment management model that changes the workflow, roles and business models sufficiently to not require regulation and intermediaries. We propose a protocol to build web3 native investment management for traditional and digital assets. Tokenization of investment strategies makes the peer-to-peer exchange of investment strategies between strategy providers and strategy users possible, and gives strategy users the possibility to automate strategy execution themselves in a decentralized way. A subscription based business model replaces management and performance fees, and thus shifts the focus away from attracting clients with the highest amount of capital to invest, to providing the best quality strategy service possible.

A permissionless model is part of the solution, but the model can only function for the benefit of all parties if trustless proof of performance forms the basis for the peer-to-peer exchange of investment strategies. It is also imperative there be clear segregation between the roles and actions of investment strategy providers and strategy users, that strategy providers have no knowledge of strategy users' investing profiles and that strategy users act exclusively on their own behalf.

We believe such a protocol provides the foundations for a minimally extractive, maximally inclusive web3 native investment management ecosystem, capable of achieving more equal distribution of wealth.

[1] Investment management, in the context in which it is used here, can also be read as fund/portfolio/asset/money/wealth management.

[2] Skeuomorphism - https://a16zcrypto.com/posts/article/tokens-are-a-new-digital-primitive/

ALPHACAPTURE
PROTOCOL

TABLE OF CONTENTS

Introduction

Investment Management

From the beginnings of the very first merchant banks, through to the sophisticated global financial markets we have today, people have always wanted to make money. That will never change. Building wealth enables a better quality of life and investment management services exist to build wealth. They allow people to put their money to work, whilst sitting back and focusing on other areas of life. Investment management provides expertise and ease. Even if people start out managing or continue to manage part of their investing themselves (self-directed/individual/retail investing), there is a natural tipping point when it becomes too time-consuming or too hard and the value of professional investment management services makes sense.

TradFi Investment Management

Maximally extractive, minimally Inclusive

We still have a system where the big money remains in traditional structures, in the same hands. Control of the highly profitable TradFi industry is concentrated in the hands of a very small number of people. Due to the heavily regulated nature of TradFi, the barriers to setting up and running an investment management business preclude all but a small percentage of people doing so. Its services to build wealth and, by extension, a better quality of life are not available to everyone. For the average investor, who does not meet the minimum investment threshold, below which it is prohibitively expensive for firms to manage clients (if maximum fees are to be extracted), these services are out of reach.

People are either dependent on a system that takes maximum fees, or they are outright excluded from it. Those excluded can invest for themselves, but despite all the advances over the last 20 years to try and make more services accessible to more people, self-directed investing services still do not come anywhere close to the level of expertise and ease offered by institutional services. And most people simply don't fall into the category of the top 3-5%, who are really successful at managing their own investing. 75% of self-directed investors lose money; they are essentially 'capital donors'[3]. Most people need the expertise and ease of professional services.

Core investment management services

At its core, TradFi investment management provides expertise and ease in the form of three key services, none of which can be accessed outside of regulated services for investing in traditional securities: (i) strategies: carefully selected investment strategies with a 'trusted'[4] proven track record of performance; (ii) execution: automated strategy execution; and (iii) custody (directly or indirectly).

[3] https://www.financemagnates.com/forex/analysis-75-of-retail-investors-are-essentially-capital-donors/

[4] In this scenario, trust has to be placed in a centralized entity, either the investment management entity itself or a third party, such as an auditor.

Investment management is built for investors. They are the primary client. Investment strategies are proprietary - either produced in-house, or sourced externally from heavily vetted strategy providers, who are essentially suppliers, and offered as the firm's own. Firms have sophisticated order execution management systems for automated execution and extensive custodial arrangements.

Proof of performance is integral to any successful investment management model
No one in the traditional, institutional world invests without proof of performance. No one. It's an established industry standard. It is a commonly accepted fact that everyone skips over the standard industry disclaimer that past performance is not indicative of future results and looks at past performance, precisely for an indication of what future results might be, to inform their decision on which investment management firm they place their money with.

Investment management firms live and die by the quality of their performance. The success of their investment strategies determines how much money firms make for and earn from their clients. They need to prove their performance record to secure the trust of their clients. They use their proven track record, typically audited by a 'trusted' third party, to attract more clients and more capital under management. The individuals at the firms who are responsible for creating high performing strategies are valued and rewarded well, really well. If a firm performs well for its clients, its clients trust them and invest more money with them. It's a virtuous cycle and on it goes. This model has been in place for a very long time, because it works.

Skeuomorphic DeFi Investment Management

Too similar to TradFi to be meaningfully different
If DeFi investment management is to offer an alternative model that can provide expertise and ease, and deliver real financial inclusion, the model cannot be skeuomorphic. It cannot use some DeFi technology, yet be a near carbon copy of TradFi investment management, but that is the DeFi model we have right now.

The DeFi investment management protocols currently available are primarily intended either for people to manage their own assets, with which we are not concerned here, or to enable a client application layer of regulated investment management businesses for digital assets; businesses that look and feel similar to TradFi investment management, because they are.

The same DeFi investment management protocols are also being used at the client application layer by services that, it would seem, do not have the intention of establishing a regulated offering; but of offering some form of investment management on behalf of others under a decentralized banner that (they hope or assume) will not need to be regulated.

Self-custody doesn't make discretionary investment management any less discretionary
What these services, both regulated and not (yet) regulated, are offering, in reality, is essentially discretionary investment management with self-custody. Whilst self-custody gives investors the option to hold their own assets,[5] discretionary investment management is still discretionary, whoever is responsible for custody, be that the investment manager or the investor.

The mechanics matter
It is important to look into the detailed mechanics of each model and what the roles and workflow reveal about the model's overall intent. Is there clear intent for the model to buy and sell assets on behalf of others with the purpose of making a profitable return, for the client and service provider; i.e. for it to be discretionary investment management?

It's too easy to assume that because a solution is labeled as DeFi, because the investment strategy is executed by a smart contract, or because someone has self-custody of their assets, or may receive tokens equivalent to the value of the investment they have made into a tokenized vault, or because they use a smart wallet etc., that the model is intended to enable people to act on their own behalf and manage their own assets, or is truly decentralized, when granular examination reveals that it is in fact discretionary and /or centralized to some extent. Analyzing the detail in the following areas, for example, is key to understanding what service is being offered and who is playing what role:

- Are there management fees for overseeing the investment fund?
- Are there performance fees for generating positive returns?
- Is the investment manager promoting strategies and encouraging people to invest?
- Is the investment manager making the decisions about what is invested in, when, how much and for how long?
- Who is accountable for the increase in value of the fund or vault?
- How decentralized is that accountability?
- If the investment strategy is an algorithm that auto-executes, who produced the algorithm?
- Can anyone change the algorithm?
- If the algorithm can be changed, are changes made in a decentralized way?
- Is the investment manager initiating the trade order execution?
- If a smart contract is triggering the trade order execution, can the smart contract be changed by the investment manager? How are the changes made? Etc.

Regulatory inevitability, not uncertainty
What service a client application is offering will ultimately dictate its regulatory path. AlphaCapture Protocol is not pro regulation for the sake of it, nor do we assume the TradFi regulatory model is the

[5] Whilst self-custody should lower administrative costs and reduce the minimum investment threshold, it will only do so to a certain extent, as costs are not the only factor driving the threshold.

only, or the best option for emerging DeFi investment management models, but we are clear in our view that, due to the nature of its design, all forms of skeuomorphic DeFi discretionary investment management will be regulated at the client application layer in some way, whether the providers of those services intended them to be or not. What we are committed to, is building a fully web3 native model that does not require regulation.

Same design, same roles, same censorship

As well as impacting the eventual regulatory status of client applications, skeuomorphic design also fails to change the roles ecosystem participants play and fails to eliminate censorship. TradFi investment management is built for investors. TradFi self-directed investing services are built for investors. Investors are their primary client. That is where the money is - the more investors and assets under management that can be attracted, the more money can be made in management and performance fees, or trading flow - and skeuomorphic DeFi investment management services are no different.

Being 'investor first' requires having the right strategies to achieve the best returns for investors, because the credibility and ultimate success of a business are dependent on it - quality strategies drive more investors to the applications and more profit. Whilst DeFi investment management should in theory open up new opportunities for strategy providers that are closed to them in TradFi, DeFi strategy providers will inevitably be subject to exactly the same kind of censorship that exists in TradFi - vetting of providers and strategies, gated access, risk limits, requirement to have trading capital and so on. Skeuomorphic DeFi investment management services are no less incentivized to hold strategy providers captive to their applications than TradFi self-directed investing services are. None of these services is designed to endow strategy providers with the tools to operate independently and interoperably across any platform.

What the skeuomorphic design of DeFi investment management means is that the service offering does not change, nor the roles, workflow or business model. The requirement to be regulated does not change and with regulation inevitably come obligations, increased costs, greater censorship and higher fees. The skeuomorphic DeFi investment management ecosystem will progressively become maximally extractive and minimally inclusive, undermining the very ethos of decentralization. The same as TradFi, but using DeFi technology. An opportunity lost.

Web3 Native Investment Management

Using digital primitives to build a new model

DeFi investment management no longer needs to be designed in a skeuomorphic way. The combined capabilities of digital primitives make it possible to design a web3 native model that changes the workflow, roles and business models sufficiently, such that intermediaries are eliminated and regulation is not required.

Non-fungible tokens (NFTs) make the tokenization of complex data – investment strategies – possible. Decentralized key management allows that complex data to be encrypted, access to it to be controlled and for the data to be decrypted and applied by those with access in a fully decentralized way.
The new model allows investment strategy providers to prove their performance track record, distribute their investment strategies directly to strategy users, and for strategy users to automate execution of

the strategies themselves, whilst maintaining complete segregation between the roles and actions of the strategy provider and the strategy user, and that the strategy provider has no knowledge of the strategy user's investing profile.

No more intermediaries
Peer-to-peer exchange of investment strategies becomes possible for any assets, traditional and digital. The permissionless investment management ecosystem that results enables anyone to provide services and anyone to access them. Communication between parties is based on trustless proof of investment performance. The performance data speaks for itself and self-regulates, removing the need for any censorship. The native DeFi investment management model is designed for investment strategy providers first, so they can operate independently and not be held captive to any platform. Strategy users have far greater and more informed choice available to them and no dependency on intermediary investment managers – they now have the power to manage strategies, execution and custody themselves directly.

Management and performance fees are dead
It is essential that the business model changes from one that focuses on how much money a client has and therefore how much can be extracted from that client, to one that focuses on the quality of the strategy service provided.

A management and performance fee model means that an investment manager can apply the same investment strategy to a client's account that has a balance of $100,000 and generate 100x the profit they do for a client that has a balance of $1,000. This is the main driver for excluding clients with smaller account balances and for seeking more valuable clients with significantly more capital to invest.

The majority of traditional investment management firms are built with the sole focus of collecting the maximum amount of assets under management possible, to earn management fees that are highly profitable, regardless of strategy performance. The change of roles and workflow in our proposed web3 native investment management model means a strategy provider has no knowledge about how much money a strategy user has, or how much profit they may generate from a strategy. It is intentionally impossible to charge management or performance fees.

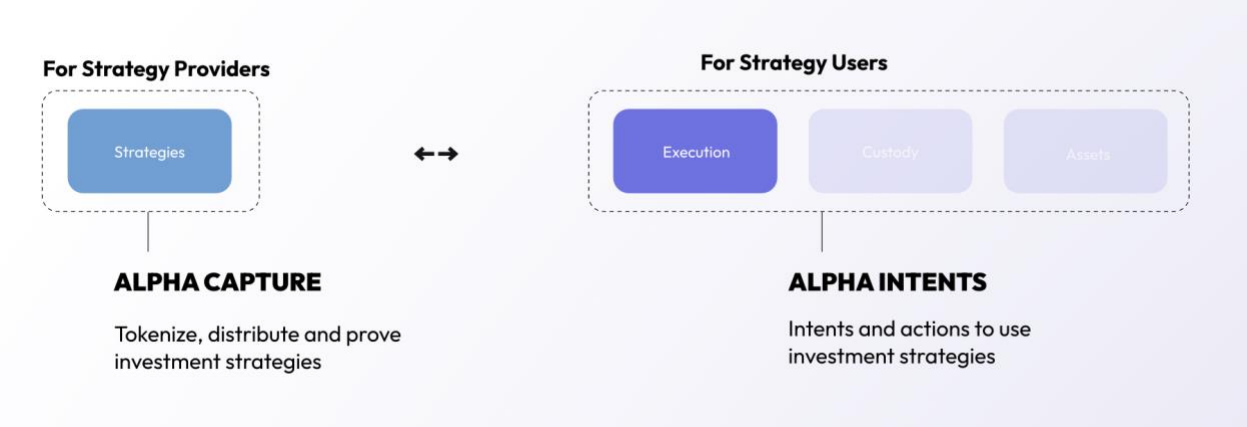
We propose a subscription based business model where strategy users pay a recurring monthly fee to the strategy provider for access to a strategy. The monthly fee is set by the strategy provider and can be correlated to their independently verifiable proof of performance record, but the amount will ultimately be determined by market forces and price elasticity. A strategy that outperforms is likely to cost more than a strategy that underperforms, while taking into account the overall number of strategy users willing to pay.

The opportunity is for strategy providers to offer their services globally, exploiting long tail dynamics. It should be entirely possible for 1,000,000 strategy users to each pay $100 per month to a single strategy provider for a quality strategy. This is minimally extractive and maximally inclusive.

This is the web3 native investment management model that provides the expertise and ease of traditional investment management, for traditional and digital assets. This is the next generation of investment management that will be used for the next 20 years and beyond.

AlphaCapture Protocol – Web3 Native Investment Management

AlphaCapture Protocol allows investment strategy providers to build applications to tokenize investment ideas or trades as NFTs, chained together as strategies, to prove ownership and performance of their strategies, and to control who can access them and at what price. Strategy providers are able to distribute strategies through their own applications or preferred channels, with no knowledge of strategy users' investing profiles. Access to strategy users is authorized through the smart contract, and they can use the Alpha Intents decentralized application (dApp), or build their own solutions to initiate their chosen action, e.g. do nothing, receive a notification, or customize automatic decentralized trade execution to any centralized or decentralized exchange (CEX or DEX).



Core Functionality

The functionality provided by AlphaCapture Protocol can be split into two distinct, but interrelated services – Alpha Capture for strategy providers, to tokenize, distribute and prove performance of investment strategies, and Alpha Intents for strategy users: intents and actions to use investment strategies.

Alpha Capture for Strategy Providers

Alpha Capture gives strategy providers tools that are interoperable across any platform and that enable them to build a business independently.

Investment strategy tokenization
Strategy providers can use AlphaCapture Protocol to tokenize investment strategies in their own back- or frontend applications. It is possible to prove ideas - a trading signal without a real trade behind it, or trades - proof a real trade took place, but a strategy can only include ideas of a single type, i.e. only proof of idea, or only proof of trade. There is no reason for ideas to be limited by capital and those who are not financially in a position to put capital at risk, yet have quality strategies, should not be automatically excluded. Using real-time market prices means having reputational skin in the game.

Each investment idea or trade in a strategy is represented on a blockchain as a unique, soul-bound NFT, using the ERC-1155 standard. The first open idea or trade created in a strategy forms the start of that strategy's performance record. All subsequent ideas or trades created in the same strategy - adjustments, closes, or new opens - are chained to the first idea in the strategy, to form the strategy's overall record. NFTs created to adjust or close an open idea are linked to the relevant NFT created for the open.

The metadata of the NFT contains the key details of the investment idea or trade:

- Open/adjustment/close position
- Direction – buy/sell
- Tradable asset
- Asset market price
- Pricing provider
- Timestamp

Smart contracts are used to validate the asset and the asset market price at the time of the NFT creation. As long as a market price can be requested from a verifiable source, such as an exchange, brokerage or pricing service provider, any asset can be supported, i.e. traditional equities, commodities, bonds etc., as well as digital assets.

The metadata of the NFT is encrypted (kept private), for open and adjust positions. The strategy provider has the option to leave it unencrypted, i.e. to make it public. A strategy provider can grant another wallet address access to the NFT, either during the creation process or at a later point. When the strategy provider grants another wallet address access to a private strategy, the wallet owner is authorized to decrypt the metadata of the NFT.

Tokenization of investment strategies opens up new opportunities for strategy providers, by unlocking capabilities in three key areas – proof of ownership of their strategies, proof of their strategy performance and control over who can access their strategies, how and at what price.

Proof of ownership
Tokenization serves as an indisputable, immutable digital record of ownership of each NFT. Strategy providers' ownership of their intellectual property is secured by a blockchain. Proof of ownership is one of the key elements that contributes to the trustlessness of peer-to-peer investment strategy exchange – that the strategy a strategy provider says is theirs can be independently verified as being such.

Proof of performance

Trustless proof of performance forms the basis on which investment strategies are exchanged peer-to-peer. It provides the requisite transparency for the proper and efficient functioning of the community, and maintains integrity of the community. Without a proof of performance record, strategy providers cannot properly monetize their strategies and strategy users lack the information to make informed decisions.

A framework for proof of performance

In an investing context, proof of performance is a simple concept - can you prove to others what your investing performance is? To prove investment strategy performance, we propose the following basic framework for what constitutes trustless proof of performance, with four attributes that must always be met.

Immutable	Once provided, the proof cannot be edited or deleted in any way.	The inherent design of blockchains provides the highest transparency with immutable data.
Independently and publicly verifiable	The proof can be verified by anyone using publicly accessible data. No contact with the party providing the proof, nor any related party, such as an auditor, is required.	The data stored on public blockchains is available to anyone, to independently verify the details and therefore be able to agree or contest the results.
Real-time	Financial markets work in real-time. Proof must also be in real-time.	The data submitted on-chain is real-time.
Sequence of events over time	An investment strategy must consist of more than one event; whilst a single trade or signal as an isolated event can be proven, it does not prove performance over time, as part of a strategy. A sequence of related events allows for proven aggregated performance.	Ideas or trades are chained together over time to provide meaningful strategy data.

Proof of idea

Strategy providers are able to prove performance of their investment ideas, using a real-time market price. A best efforts approach is offered - the market price at the time of the request is the closest price to what an execution price would be in real-time. There is no concept of order size when creating an investment idea and so it is not possible to allow for slippage. Proof of trade can be used instead, or the raw strategy data can be used to calculate performance allowing for a wider spread. When a strategy provider creates an idea, a market price is requested by the strategy provider from a supported pricing provider (brokerage, exchange or pricing service). Ideas can only be created when the relevant market is open.

Obtaining a market price

The price at which an investment idea is opened, adjusted and closed is one of the most important attributes of any trading signal and proving this price is a key part of AlphaCapture, so that there is trustlessness in the price – transparency where the price comes from and that it has not been or could not have been tampered with. Even if the price comes from a centralized service which has to be 'trusted', the key is to communicate in a trustless way where the price came from, at what exact time and at what exact price.

The strategy provider specifies their preferred pricing provider - this could be a CEX or DEX, brokerage or pricing service provider. During the NFT creation process, a request is made to the specified pricing provider. We use Lit Protocol (https://litprotocol.com/), who offer Lit Actions, which provide a distributed oracle equivalent. Multiple nodes in the distributed network are randomly selected and make the call to the pricing service at the same time. All nodes must make the call within a specified time window. The returned pricing data from the nodes is shared, merged, validated, signed and submitted with the idea request. The signing process ensures that the data cannot be altered.

In order for proof of an idea to be as close to real-time trade execution as possible, the same pricing provider used when creating the idea, must be used again when subsequently adjusting or closing the idea. It is not possible to use one pricing provider to open a new investment idea and another provider to close the same idea, because this would compromise the proof of performance record.

Proof of trade

Proof of Trade is proof that a real trade took place on an exchange or at a brokerage. The process for proving a trade is similar to proving an idea – the trade is taken as a signal, except that the price used is that at which the trade was executed.

Proof of Trade allows strategy providers to prove historical trades. Smart contracts and oracle type services are used to request data on behalf of the strategy provider. As long as the data can be requested from the exchange or brokerage (via API), there is no limit to how old a trade can be. Older or newer trades can be added at any time and as far back as possible, however the trade added must always be n+1 or n-1. This means there cannot be any gaps between trades. The trades in a proof of trade strategy must all come from a single exchange or brokerage.

Encryption

The decision whether the strategy will be private or public will be determined by the strategy provider's specific use case. When creating NFTs for open or adjustment positions, the metadata of ideas or trades is encrypted, but strategy providers are able to specify if they wish to leave them unencrypted and make them public, and therefore whether only authorized wallet owners or anyone is able to decrypt the metadata. Encryption enables strategy providers to keep sensitive data and their intellectual property protected. A primary example being time sensitivity of when to open a position – valuable data the strategy provider may want to monetize.

The strategy provider can set strategy access authorization as public or private, as well as edit the authorized wallet access list at any time. It is possible to create private ideas or trades on a private strategy and later make them public or accessible to another wallet(s). For private strategies, unless a

strategy provider specifically shares their strategy with AlphaCapture Protocol, AlphaCapture Protocol never has access to any of the encrypted NFTs, only the publicly available ones.

Trustless public performance record
By default, all close positions are made public. This is necessary in order to create a trustless record of performance that can be independently verified by anyone without the need for any intermediary. This means that it is then possible for anyone to view the data on-chain, calculate and verify the performance of an idea or trade, and of the overall strategy. As the idea close is chained to the idea open and any adjustments, it contains details of all the idea stages, enabling calculation of the investment idea performance and verification of key details, such as asset, prices and timestamps.

It is not possible to delete or alter a performance record on-chain. It is our belief that such levels of transparency will drive a greater level of accountability and result in significantly improved access to investment strategies with a proven track record for average investors. We also believe that the value of proof compounds and that by enabling strategy providers to build a record of their investment performance that can be lifelong, they are able to monetize their intellectual property at a price point correlated to their performance.

Access control
Tokenizing ideas or trades enables strategy providers to control who can access their strategies, how and at what price. When an idea or a trade is tokenized as an NFT, the strategy provider can pass in the wallet address of a person, group, company, entity etc. with whom they want to share their strategy, and the strategy will be shared with that wallet address. There is no limit to the number of addresses that can be passed in.

The wallet address holder that is the recipient of the idea or trade NFT is recorded in the strategy access list on the smart contract. If a strategy provider grants a wallet holder access to an idea or trade open, the wallet holder will automatically receive access to any subsequent adjustments, unless access is revoked. As close ideas are always public, the wallet holder is always able to access them.

Access control unlocks the ability for the strategy provider to share their strategies securely at scale, privately or publicly. It is up to the strategy provider if they want to share their strategies for free, or if they want to monetize them and charge a recurring subscription fee for access.

Investment strategy distribution
Strategy providers are able to share their strategies for free, if they wish, but one of the primary benefits unlocked by tokenizing investment strategies and proving strategy performance is the ability for the strategy provider to monetize their strategy at a price point correlated to their proven performance. Strategy providers have the ability to set their own recurring subscription price and to distribute their strategies through any channel they wish to.

It is imperative there be clear segregation between the roles and actions of investment strategy providers and strategy users, that strategy providers have no knowledge of strategy users' investing profiles and that strategy users act exclusively on their own behalf. To this end, strategy providers are able to distribute their strategies through a 'no-knowledge' on-chain subscription (nKSubscription).

nKSubscription
The nKSubscription enforces the two segregated roles: (i) strategy providers sell access via authorized access control to their investment strategies; (ii) strategy users are responsible for their own investing decisions.

The strategy provider:

- only knows the wallet address of the strategy user
- has no knowledge of who the subscribing strategy user is, other than the wallet address
- has no knowledge of any aspect of the strategy user's investing profile
- has no knowledge of the strategy user's portfolio
- has no knowledge of any connected brokerage or exchange accounts the strategy user may have
- has no knowledge of the strategy user's risk appetite or goals
- has no knowledge of whether the strategy user is executing any trades based on the communicated investment ideas or trades
- has no knowledge of whether the strategy user does or does not profit from the communicated investment ideas or trades
- does not manage money on behalf of the strategy user
- is not advising the strategy user on their investments
- is not executing trades on behalf of the strategy user.

Equally, the strategy user:

- never shares any personal or financial information with the strategy provider
- never connects a brokerage or exchange account
- never shares API keys, security tokens or any other type of access which may give the strategy provider access to their investments
- is not required to ever send money, of any type, to a service offered by a strategy provider

Alpha Intents for Strategy Users

The Alpha Intents dApp gives strategy users the tools to be able to use investment strategies to which they have access, independently of any intermediary. It allows them to initiate their chosen action, which could be anything from, do nothing, receive a notification, or customize automated strategy execution to any CEX or DEX. All logic for the intents is accessed via the strategy user's wallet, using a decentralized database. Alpha Intents uses distributed and decentralized technologies to process the intents defined by strategy users. Intents and actions can only ever be initiated by the strategy user.

Alpha Intents is open source, to allow for anyone to adapt or contribute to the Intents and Actions that anyone in the community might want to use. Only through open source can the scale of Intents and Actions be reached, i.e. all CEX/DEX exchanges globally and all notification services.

Intents
Strategy users state what they want to do when an idea or trade NFT is issued within a strategy.

Examples are:

- Do they want to do anything or do nothing? If anything:
- Do they want to receive a notification to Slack, Telegram, Discord etc.?

- Do they want to automate trade execution?
- To which CEX or DEX account do they want to automate execution?
- Do they want to do so without making any modifications to the order size as recorded in the metadata of the NFT?
- Do they want to customize the order size, allowing for leverage, maximum position size, and existing portfolio allocation?

Event listeners
The event listener listens in real-time for an idea or trade NFT to be issued in a strategy to which the strategy user has authorized access. On receipt of an idea or trade NFT, the event listener processes the intent(s) stated by the strategy user and triggers the resulting action(s).

Decryption
The event listener calls the AlphaCapture Protocol software development kit (SDK) to trigger decryption of the metadata of the NFT and retrieves any required credentials from the strategy user's wallet for automated decentralized trade execution, using smart contracts and/or Lit Actions (oracles).

A strategy user can, initiated by a wallet based authentication request, use the Alpha Intents dApp, AlphaCapture Protocol SDK or any other dApp supporting the AlphaCapture Protocol, to trigger decryption in the same way.

Decentralized order execution management
A strategy user is able to initiate automated trade execution to any CEX or DEX. A strategy user's credentials for their CEX or DEX account are stored as an encrypted NFT, secured via their wallet.

At no point does a strategy user connect their brokerage or exchange account to the strategy provider for trade execution. The authentication details are encrypted as an NFT, secured by the strategy user's own wallet. No data, credentials, API keys, account details or portfolio details are ever shared with any other party, including strategy providers or AlphaCapture.

This is important for several reasons:

- The signal generation and the execution layers are completely separated
- Trade order execution is configured entirely by the strategy user as the responsible party
- The strategy provider has no knowledge of what the strategy user does with the idea or trade NFT after they receive it
- The strategy provider has no knowledge of the strategy user, their portfolio or their investing profile
- The strategy provider is not advising the strategy user in any way
- The strategy provider is not initiating trade execution or managing money on behalf of the strategy user.

How AlphaCapture Protocol and Alpha Intents Work Together

An example of the complete flow of AlphaCapture Protocol and Alpha Intents.

Alice is a strategy provider

- Alice has an investment idea that now is a good time to buy NVIDIA.
- Alice specifies NVIDIA as the tradable asset, for which she wants to request a price and the IEX Exchange as the pricing provider she wants to use.
- The NFT for the idea records on a blockchain that the open idea was to buy 1 share of NVIDIA on 22nd May 2024 at 12.00 for a price of $95.00.
- Alice then decides to close her position.
- Alice specifies NVIDIA as the tradable asset, for which she wants to request a price and the IEX Exchange is automatically used as the pricing provider, having been used for the idea open.
- The NFT for the idea records on a blockchain that the close idea was to sell 1 share of NVIDIA on 6th June 2024 at 12.00 for a price of $125.00.
- The open and close ideas are chained together and the close idea is made public.
- Anyone can independently verify that Alice made a theoretical profit of $20.00, or ~31.5%.

Bob is a strategy user

- Bob has subscribed to Alice's investment strategy.
- Bob has configured his Intents to state that when NFTs from Alice's investment strategy are received, he wants to automate the execution of the ideas into his TD Ameritrade account.
- As part of the configuration, Bob specified that any new positions should be 1% of his portfolio value at the time of order placement, taking into consideration the maximum position size, existing portfolio and other factors such as leverage preference if applicable.
- The Alpha Intents event listener detects on 22nd May that a new NFT from Alice's strategy has been issued.
- The event listener calls the AlphaCapture Protocol SDK to trigger decryption of the metadata of the NFT and also retrieves Bob's TD Ameritrade account credentials from his wallet.
- The event listener processes Bob's stated intent and triggers automatic trade execution to buy a 1% position of NVIDIA.
- The Alpha Intents event listener detects on 6th June that a new NFT from Alice's strategy has been issued.
- The event listener again calls the AlphaCapture Protocol SDK to trigger decryption of the metadata of the NFT and retrieves Bob's TD Ameritrade account credentials from his wallet.
- The event listener processes Bob's stated intent and triggers automatic trade execution to close his position in NVIDIA.

AlphaCapture Tech Stack

AlphaCapture Protocol

AlphaCapture Protocol is built on Ethereum Virtual Machine (EVM), and uses Solidity, InterPlanetary File System (IPFS) for storage and offers Node SDKs. The protocol has a set of smart contracts, for tokenization of investment ideas or trades and for nKSubscription.

Lit Actions are used for obtaining prices, and Lit Protocol for signing of the price using their decentralized key management, as well as for access control, for strategy providers to grant access to their strategies. We also use Lit Protocol's signing and decentralized key management for encryption and decryption of the NFT metadata.

We offer two versions of the SDKs – one for backend and one for frontend integrations.

Alpha Intents

Alpha Intents is an open source dApp, currently built with Angular and Node. It uses AlphaCapture Protocol's SDK to retrieve idea or trade NFT data and WeaveDB, a decentralized database (https://weavedb.dev/), to store intents. Processing of intents is intent specific. For example, Node is used for Slack notifications and DEX execution; Lit Actions for CEX execution etc. Lit Protocol is used for encryption and decryption of credentials NFTs, using their signing and decentralized key management.

Our definition of intents is broader than the commonly understood definition of web3 intents. In addition to on-chain intents, we also use off-chain intents. For us, stating an off-chain intent is no different in purpose to stating an on-chain intent, though the exact path to realizing the intended outcome will differ from an on-chain path.

Alpha Intents is provided as an open source application to encourage support for the greatest range of Intents.

Use Cases and Applications

Investment Strategy Types

AlphaCapture Protocol can be used for any type of investment strategy, TradFi or DeFi, provided a live market price for the tradable asset can be obtained.

It's worth looking briefly at the different types of investment strategy that exist and the different meanings of alpha in TradFi and DeFi. The type of investment strategy that a strategy provider is using will determine if tokenizing their strategy, proving their performance and monetizing it through distribution to others suits their objectives. Broadly speaking, there is a use case for any TradFi strategy and most DeFi strategies.

We chose AlphaCapture as our name for a reason. In TradFi, alpha generally refers to the ability of an investment strategy to outperform the market benchmark. Since the creation in 2001 of Marshall Wace's TOPS (Trade Optimised Portfolio System), the first alpha capture system, the big institutional TradFi players all have sophisticated alpha capture systems. Sell-side firms around the world submit their investment ideas (accompanied by a rationale, timeframe and conviction level) into these systems, which use algorithms to analyze and optimize the information to try and achieve market-beating returns, and to monitor the performance of submitted ideas.

In TradFi, investment strategies are generally specific market trading strategies - systematic methodologies for buying and selling assets, typically based on pre-defined rules and criteria. A strategy may be simple or complex and involve considerations such as investment style (e.g., value vs. growth), market cap, technical indicators, fundamental analysis, industry sector, level of portfolio diversification, time horizon or holding period, risk tolerance, leverage, tax considerations etc.. Most alpha in traditional markets comes from four key sources – behavioral, information, analytical and technical.[6]

Whilst an analytic edge is a source of alpha in any market and DeFi is no different - DeFi is an incredibly data-rich market with data sets available on public blockchains - alpha in DeFi can mean something quite different. It isn't necessarily related to following a specific market trading strategy, as in TradFi. This is for two primary reasons – it is harder to benchmark performance of the DeFi market and the unique characteristics of DeFi translate into native sources of alpha that have not existed before – infrastructure, protocol, governance and information alpha - and therefore into different types of investment strategy.

Alpha in DeFi takes many shapes and forms, but most of the time, it can mean everything from achieving alpha returns by hosting validator or staking nodes without having to execute a specific market trading strategy, hunting for new protocols and tracking their launch, monitoring and taking advantage of governance proposals that alter things such as liquidity incentives, to benefiting from the asymmetry of information that exists in an unregulated, inefficient, early stage market, for example, by being close to new protocols and information on their token distribution model, launch schedules or governance proposals.

Strategy Provider Types

We see initial use cases for strategy providers with strategies for both traditional and digital assets, and their respective followers or subscribers, strategy users. We solve the various challenges all of these parties face today.

User: TradFi Strategy Providers outside of the regulated investment management industry
Use Case: prove performance and monetize strategies independently

Centralized services inherently limit the reach and earning potential of strategy providers. They will never be able to offer the solutions that these strategy providers need to monetize their strategies; only a web3 native solution can.

50% of investors[7] now source investment strategies online instead of using traditional services, but the majority of strategy providers share their strategies for free, due to their dependency on centralized parties and the respective associated constraints. These strategy providers lack ownership and control. The centralized services determine the entry criteria and business model, they own the strategy provider's data, users and performance record, if it is possible to build one.

[6] https://macro-ops.com/wp-content/uploads/2019/02/Who-Is-On-the-Other-Side.pdf

[7] https://www.finrafoundation.org/sites/finrafoundation/files/NFCS-Investor-Report-Changing-Landscape.pdf

The specialist tools are also lacking. Social media posts, newsletters or chat rooms are not designed for sharing often complex investment strategies at scale, and they offer strategy providers no way of protecting and meaningfully monetizing their valuable intellectual property. Proving performance, which is the key enabler to proper monetization of investment strategies, is hard on centralized services. The options open to strategy providers are poor[8] and a hard-worked for performance record can disappear overnight if a service stops.

We use our proof of performance framework to analyze the options available today - social media, centralized copy trading brokerages, third party auditors or services that use brokerage or exchange account connections.

Any social media		
Immutable	Posts can be edited or deleted by the author; they are not immutable. As centralized services, centralized networks own any data posted to them and are able to restrict access to it at any point – to the person posting or to anyone viewing.	Fail
Independently and publicly verifiable	The data contained in the post cannot be precisely verified, nor is there any consistency across posts to provide a common data structure that could provide a way to verify strategy performance: • If a trade, there is insufficient data or means to prove that this actually happened. • If an idea, there is insufficient data to indicate the validity of the price or even the asset.	Fail
Real-time	Posts can be posted in near real-time.	Pass
Sequence of events over time	Posts are largely independent events. It is possible, of course, to create a chain of posts by replying to a previous post, but there is no enforcement of this sequence nor immutability, therefore the sequence can be easily broken at any point.	Fail

Centralized copy trade brokerage/exchange		
Immutable	While practically it is difficult for an author to modify data, the data is held by centralized parties and is therefore not immutable. It requires trust in those parties not to modify the data and to represent it as it was intended. Those parties may restrict access to it at any point – to the account owner or anyone viewing it.	Fail

[8] https://io-fund.com/finance/financial-analysis/the-importance-of-verified-returns-and-risk-management-2024

Centralized copy trade brokerage/exchange (cont.)		
Independently and publicly verifiable	Data is not publicly verifiable and requires the consent of the account owner and/or centralized parties to grant access.	Fail
Real-time	Trades can be created in real-time.	Pass
Sequence of events over time	Strategies can be created as a sequence of trades (where a trading account represents that strategy).	Pass

Third Party Auditor		
Immutable	Data and reports provided by an auditor are not immutable.	Fail
Independently and publicly verifiable	Verification is provided by the auditor who must be trusted. Data cannot be independently verified.	Fail
Real-time	There is typically a lengthy delay (weeks or months) between the trades and verification.	Fail
Sequence of events over time	Performance is recorded as a series of trades over time.	Pass

Centralized services using brokerage or exchange account connections		
Immutable	The strategy provider or the account connection service could disconnect the account at any time. The account connections are reliant on centralized parties that hold the data. Trust is required that those parties will not modify the data and will represent it as it was intended. Those parties may restrict access to it at any point.	Fail
Independently and publicly verifiable	Data is not publicly verifiable and requires the consent of centralized parties to grant access.	Fail
Real-time	Whilst trades can be created in real-time, the services using brokerage or exchange account connections typically have a time lag between trade execution and account positions updating, anywhere between 10 minutes to 24 hours. They are reliant on brokerage or exchange APIs not originally designed for that purpose and sometimes also third party connection services that only pull data periodically or end of day.	Fail

Sequence of events over time	Strategies can be created as a sequence of trades.	Pass

None of these is trustless and they all come at a cost – whether that be financial, privacy, security or time. Due to the constraints of regulation, copy trading brokerages or exchanges are the only option for strategy providers in TradFi to monetize their strategies. Only these services have the tools to create a real-time performance record and the regulatory licenses to enable automatic strategy execution for followers. That is a very limited segment of the market.

User: Digital asset strategy providers
Use Case: Protect and monetize intellectual property

In DeFi, strategy providers are able to point to their trades on a blockchain that are immutable, independently and publicly verifiable, and real-time, but the raw trade data on a blockchain is not chained together over time as a strategy. Nor does a wallet in itself provide strategy context. The purpose of a wallet is different to the purpose of an investment strategy.

Wallets have many purposes, not just pursuing trading strategies, such as withdrawals, paying funds to other parties, or one off trades that don't form part of a specific strategy. The strategy user will know the intent of each transaction, but a potential strategy user does not, so whilst there is nothing stopping either party from collating the aggregate performance of a wallet, that is not the same thing as a trustless proof of performance record that can be directly linked to a strategy. A strategy provider would potentially also have to prove multiple times in an easy, scalable way that the relevant wallet address and therefore the associated ideas or trades are indisputably theirs.

A strategy provider is also able to execute their strategy in a vault for anyone to see and follow in real-time. A vault should provide the strategy context that a wallet alone cannot and many of these do come with monetization options for strategy providers, but almost exclusively in the skeuomorphic form of management or performance fees. And what they are essentially providing is a form of discretionary investment management.

The reality of open ledgers and pseudonymous blockchains makes it challenging for digital asset strategy providers to protect their trades as their intellectual property[9]. Alpha, market out-performance, is by definition the exception, not the rule. Those with alpha therefore typically want to protect it. If they were to give it away, it would no longer be alpha. Without tokenization, strategy providers do not have the option to encrypt and protect valuable intellectual property, and lose out on opportunities to monetize it, as trades or ideas.

Whilst transparency is intrinsic to decentralization and publicly verifiable distributed ledgers are a key contributor to enabling a web3 native investment management product, they do not amount to an investment management product in themselves.

[9] https://blog.pantherprotocol.io/alpha-protection-through-privacy-a-web3-privacy-primitive-for-defi/

Strategy Users

User: Self-directed investors (strategy users) in TradFi or DeFi
Use Case: Access strategies with a proven track record and automate execution

For self-directed investors managing their own investments and sourcing their investment strategies online themselves (that is now 50% of people[10]), there is a lot of noise and, with no proof of performance standard, it is very hard to know who to trust and which strategies are actually any good. There is incredibly low accountability in terms of proof of performance offered to self-directed investors. The majority are not able to make investment decisions informed by a proof of performance record they can trust. Even then, replicating a strategy is almost exclusively a manual exercise that is time-consuming and challenging in terms of time sensitivity of trade execution. Centralized or decentralized copy trading brokerages or exchanges, or bots are the only option to find strategies with a proven track record and that offer real-time strategy automation. Each option comes with its own limitations for strategy users, however.

In DeFi, whilst it is possible to automatically copy trades executed by another wallet in real-time and in a fully decentralized way, using decentralized copy trade bot services, a wallet is not synonymous with a strategy and does not provide aggregate strategy performance, as we have outlined.

In using the copy trade services of centralized brokerages or exchanges lies an inherent contradiction – your broker is not your friend; your broker takes the other side of the trade. Most offer copy trading for free, because it is a way for them to attract more users and make more money through trading flow. Fifteen years in and copy trading only constitutes 3% of copy trading brokerages' total traded volume.[11]

For any service, centralized or decentralized, it is only possible to copy the strategies or trades of those providers or wallets available on that service. It is not possible for a strategy user to simply choose any strategy they want from anywhere and apply it to any account they want.

Other

User: Investment strategy marketplaces
Use Case: Earn subscription revenue; attract new and retain existing users with a new value proposition

Once the atomic network of strategy providers is sufficient at the client application layer, there is a clear use case for development of investment strategy marketplaces. This could equally be built by a new marketplace provider, or by an existing service that already has a relevant captive user base, such as a financial news site or an online investing community.

[10] https://www.finrafoundation.org/sites/finrafoundation/files/NFCS-Investor-Report-Changing-Landscape.pdf
[11] https://www.financemagnates.com/forex/technology/with-only-3-of-total-traded-volume-is-social-trading-dead/

In this scenario, the marketplace would earn a share of revenue from no-knowledge on-chain subscriptions and the strategy providers would automatically gain exposure to a far larger audience than they are able to reach on their own.

We will open-source a dApp to pull public strategy performance data, to allow for anyone to build a marketplace.

User: Regulated digital asset businesses
Use Case: Prove performance to attract clients

Digital asset trading is still in its infancy and new entrants to the market are often not able to evidence several years of investment performance history, but they need to prove their performance in order to attract new clients. They need an on-chain solution that allows them to protect their alpha, and flexibly and immediately market their services at scale through any channel.

It is cheaper, easier and real-time for them to prove their investment performance by tokenizing their trades or ideas, rather than using an often expensive, centralized third party auditor that has a minimum time lag of a quarter or more. To have to prove performance using a centralized web2 service feels anachronistic when operating in on-chain world.

Community Incentives

As a permissionless community, no one is excluded. All community members share an overarching and aligned economic incentive to build wealth. Sharing is also built into the product, primarily in the form of strategy subscriptions. A web3 native model unlocks real utility for strategy providers and strategy users, and community incentives are inherent in the utility AlphaCapture Protocol and Alpha Intents provide. It is the real utility that enables the proper and efficient functioning of the community, and drives growth in the value of the community.

For Strategy Providers

AlphaCapture Protocol unlocks several areas of real utility for strategy providers and at a minimal cost, through tokenization and nKSubscription.

Proof of ownership
Real utility: An immutable, indisputable and publicly verifiable digital record of ownership of each NFT secures a strategy provider's intellectual property. Intellectual property can be either ideas or trades, meaning there is no capital barrier.
Community incentive: Proving ownership creates trustlessness for strategy users to use strategies, which is fundamental to adoption and growing the community.

Proof of performance
Real utility: An immutable, publicly verifiable record of investment performance history, for any asset class, for trades and for ideas.

Community incentive: Proving performance creates trustlessness. It opens up monetization opportunities to distribute investment strategies at a price point directly correlated to the strategy provider's performance history and, should performance improve, it opens up the opportunity to increase the value of the subscription price and potential subscription revenue. Value of proof compounds over time – the longer the performance record, the more valuable it becomes. Promoting good performance drives potential growth of subscription revenue, whether done by strategy providers directly or by strategy marketplaces.

Encryption and access control
Real utility: The ability to protect intellectual property and share it in a secure, scalable way.
Community incentive: Secure and monetize valuable intellectual property; increase potential reach through a sharing model that scales.

Usability for strategy users
Real utility: Tokenization makes it possible for strategy users to apply strategies on their own, either using Alpha Intents or other dApps that support the AlphaCapture Protocol.
Community incentive: For strategy providers to educate their communities on the benefits of using strategies tokenized with the AlphaCapture Protocol, to drive usage of Alpha Intents or open source creation of other similar dApps to expand the ecosystem of available services.

nKSubscription
Real utility: Distribution and monetization of investment strategies securely at scale to strategy users, without any knowledge of their investing profiles.
Community incentive: Distribute investment strategies to the largest audience possible, to maximize revenue opportunities.

For Strategy Users

Alpha Intents unlocks real utility for strategy users to access and use strategies independently of any intermediary, to build wealth.

Proof of performance
Real utility: Quick and easy access to investment strategies with independently verifiable performance records.
Community Incentive: Use performance records to make more informed decisions about their investing at no financial cost.

nKSubscriptions
Real utility: Freedom of choice to subscribe easily and securely to investment strategies with an independently verifiable performance record, without having to share any personal data or credentials, and at accessible price points.
Community Incentive: Subscribe to access strategies that could deliver a profitable return.

Intents, event listeners and decentralized order execution management
Real utility: Ease and flexibility for strategy users to use the strategy they want to, the way they want to and in the account they want to, independently of any intermediary, and at a minimal cost.

Community Incentive: Use automatic execution to ensure time sensitive application of strategies to try and achieve a profitable return.

Community Access

Access to the community is granted through ownership of idea or trade NFTs tokenized using the AlphaCapture Protocol. Strategy providers own the NFTs of the ideas or trades they create. Strategy users who have authorized access to the strategies can prove the active period of their strategy subscription through immutable timestamped events on the smart contract. Ownership of the NFTs unlocks other benefits, such as events or discounts for related services, and airdrops for future AlphaCapture native tokens that reward contribution towards growth in the value of the community.

AlphaCapture Token

We expect to plan for the launch of an AlphaCapture fungible token and that timing be closely aligned with achieving product market fit.

Tokens would be used to reward core contributors in the AlphaCapture community – strategy providers, strategy users and strategy marketplaces - for contribution towards growth in the value of the community. Token rewards work in tandem with the incentives triggered by the real world utility enabled by AlphaCapture Protocol and Alpha Intents.

In order to incentivize the right behaviors from the right type of users, rewards are to be allocated commensurate with growth achieved and to be metrics based only. Example areas where token incentives could be used are: profitable strategy performance, longevity of proof of performance record, and number of active strategy subscriptions.

For example, a token reward could be paid each month to strategy providers on a per strategy basis, if the following criteria were to be met:

- Profitable strategy - being profitable has clear direct benefit to the community
    - The strategy must have been running for longer than 3 months.
    - The strategy must have been profitable for the prior 3 months on a rolling basis.
    - If the strategy has been running for over 12 months, then it must be profitable over the prior year.
    - The strategy must be profitable over its lifetime.
- Longevity - the number of months a strategy has been active is important; the longer the better
    - Rewards could be allocated for different periods of longevity, e.g. 6 months, 12 months, 18 months, 24 months etc.
    - There must have been a least one idea or trade during the month to ensure that the strategy hasn't been stopped.
- Active strategy subscriptions
    - The number of subscribers must be increasing over:
        - A rolling 3 month period.
        - Per annum.

- nKSubscriptions must be enabled.

Given power laws, there are likely to be a very small number of strategy providers who are rewarded with tokens each month.

There could also be scenarios where tokens are allocated to strategy providers to enable them to reward their top strategy users, for example, for longevity of subscriptions or user referrals that grow their communities.

The native token will unlock community benefits for holders.

In time, these rules would be passed to a decentralized autonomous organization (DAO), so that they can be adjusted without a centralized party.

Conclusion

Building wealth enables a better quality of life. It should be a right, for everyone. Traditional investment management enables people to build wealth. Professionals manage assets for others and provide expertise and ease, but as an ecosystem that is maximally extractive and minimally inclusive, it is off limits to the average investor, to most people.

If you were to start from first principles and build a new investment management ecosystem, open to anyone, you would build it differently to the system we have today. Yet, DeFi investment management alternatives to date are designed on traditional, centralized models. They are skeuomorphic. They will become like the system we already have, the exact system DeFi is trying to change. They will miss the opportunity to build a new model that makes investment management accessible to anyone and will fail to deliver on DeFi's promise of financial inclusion.

Web3 native investment management is that new model, for traditional and digital assets. Digital primitives make it possible to design a model that is fully decentralized, permissionless, censorship resistant and that does not require regulation. A model that is minimally extractive and maximally inclusive.

We have proposed a model for web3 native investment management, through the peer-to-peer exchange of tokenized investment strategies for digital and traditional assets, with applications at the client layer for anyone to use those strategies as they want. The model is based on trustless proof of performance as the standard for exchange and uses an nKSubscription for complete segregation between the roles of strategy providers and strategy users. It incentivizes strategy providers to provide the best quality strategy service possible.

It is a model based on transparency and accountability, privacy and security. Control, value and integrity. It enables freedom of choice and brings equality of opportunity to provide and access services, to drive greater equality of wealth distribution in the world.

This is not an incremental change in investor choice, but the opportunity for a fundamental shift of control away from centralized institutions to individuals. It is a new ecosystem that will take shape and take hold over the next twenty years and beyond. And be a force for good in the world. This is the ecosystem AlphaCapture is building.